PCT / IB 04 / 51066

Europäisches Patentamt

European Patent Office

Office européen des brevets

Bescheinigung

Certificate

Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

03101998.7

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Europäisches Patentamt
European Patent Office
Office européen des brevets

Anmeldung Nr:
Application no.: 03101998.7
Demande no:

Anmeldetag:
Date of filing: 03.07.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Secure indirect addressing

In Anspruch genommene Prioriät(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04L29/06

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT RO SE SI SK TR LI

Secure indirect addressing

The invention relates to a method of communication, comprising the steps of a sender device transferring a communication fragment to a router device, the communication fragment comprising a first target address reference referring to a target device or group of at least one target device and the communication fragment being at least partly protected by a MIC, the router device forwarding and optionally modifying the communication fragment for each target device, the router device subsequently transferring the modified communication fragment to at least one target device. The invention further relates to the corresponding sender device, receiver device, router device, and system.

In communication networks often the distinction is made between unicast, multicast and broadcast. Unicast is the situation where a single device (the sender device) sends a message to a single other device (the target device). In multicast, the sender device sends a message to a number (more than one, but not all) of target devices while in broadcast, the sender device sends a message to all devices in the network.

While nearly all networks contain routing algorithms that support unicast, this is not always the case for multicast. When multicast is not supported by the routing algorithms and a single device still wants to address several devices, multicast can be achieved by repeated unicast.

However, the sender device might not be able or allowed to do repeated unicast due to, for example, power or cost constraints. An example is a wireless control network used to control lights in large public spaces. Here a single, cheap light switch must be capable of switching more than, say, 50 lights. It is obvious that many more application examples can be found.

A solution to this problem can be found in indirect addressing (IA). where a second device (the router device) is available in the vicinity of the sender device. The sender device will then send a single message to the router device which will than do the repeated unicast.

However, problems might occur if we consider security aspects of IA. For example, the application running on the sender device might want to encrypt its message using a cryptographic key K_G known only to members of G. Further the sender device might want to apply a Message Integrity Code (MIC) on parts of the communication such as its own address ID1 and the destination address G in the message also using K_G. The result is that only the members of G (but *not* the router device) can read the message and receiving devices can verify if indeed the message is intended for them and if it was sent by the sender device ID1.

Communication protocols are commonly described using a layered, OSI-like stack. From bottom to top, the physical layer (PHY), the medium access control layer (MAC), the network layer (NWK) and the application layer (APL) are part of this stack. Roughly speaking, frames exchanged between equal layers on different devices consist of a *header* and a *payload* and a frame at level *n* in the stack is physically sent as the payload of a frame at layer *n*-1.

The abbreviations are as follows:

1. SRC: source address
2. DEST: destination address
3. INF: information field

A straightforward but inefficient solution to the problem would be to have the application compute a MIC on the message and its destination and source address using the group key K_G.

The NWK layer will then also add the NWK-DEST and NWK-SRC addresses, as they are usually required by the routing algorithms. It further might compute an additional MIC on these two NWK addresses. As compared to the solutions given above this will result in more overhead (one or two more addresses) and one MIC to be sent which makes this solution less efficient. A second drawback is that the APL level is concerned with verifying addressing information, a task which more naturally belongs at a lower layer.

Is therefore an object of the invention to provide a method that improves the efficiency of indirect addressing while providing security.

This object is realized by the invention according to the claims.

In many cases there is a close relation between the addresses at the APL layer and at the NWK layer which makes it possible to leave out duplicated address information in the APL layer in order to arrive at an efficient solution (address information at the NWK layer can usually not be omitted because it is required by the routing algorithms).

Because the APL addresses are usually equal to the NWK addresses or can be derived easily, they are not always present in order to reduce the size of the message. The INF fields contain information for a receiving device on the different layers on what kind of information is present in the rest of the message and how it should be treated. For example, the MAC-INF field might indicate that the MAC-PAYLOAD is encrypted. This will show to the receiving device that it must first decrypt the payload before dealing with it further. Also, the NWK-INF field might indicate that the received frame is generated in the context of indirect addressing and should be treated accordingly.

It is important to note that the application running on the sender device does not trust intermediate nodes (including the router device) with its address and message information and hence the addressing information should be protected with a MIC using the key K_G. However, the router device should be able to change the addressing information in order to do repeated unicast. Obviously, since G is protected by the MIC, it cannot simply be substituted by a target device address to do repeated unicast: when the target device receives the communication fragment with the substituted address and it checks the MIC, it will find a mismatch because the protected information should contain G and not the target device ID. As a result, it will probably ignore the message.

The router device therefore indicates the usage of indirect addressing by for example setting a special IA bit field in the message. The addresses MAC-DEST and MAC-SRC indicate that a message is sent from ID1 to ID2. The addresses NWK-DEST and NWK-SRC indicate that the final destination of the message is all the members in G (possibly except ID1 itself) and that the message was sent by ID1. The NWK-INF field further indicates that we are dealing with a message in the context of indirect addressing (IA=1) and the application on ID1 encrypted the string m using the group key K_G (indicated by $E_{KG}(m)$).

On receipt of the message from the sender device, the router device notices that it is an IA message by inspecting the IA bit in the NWK-INF field and it will perform a multiple unicast to all the members of G (possibly except the sender device ID1).

We will now focus on the unicast message send by the router device to the target device. From its routing information (e.g. routing tables), the router device knows that a way to reach the target device is sending it to intermediate nodes. The router changes NWK-DEST field from the entry G to the target device ID, as intermediate hops are not aware of a group identity G and the unicast routing algorithms need a single, known device address as a final destination. Note further that, because of the replacement, the MIC and the protected information are no longer consistent. The target device upon receiving the message will replace the modified information, for example the target device ID by the group ID, and is thus able to verify the MIC. The target device may know the identity of all devices in G in order to perform this action. An alternative solution is that the sender device or the router device copies the group identity G in the NWK frame, for example in the NWK-INF field. This way the target devices do not have to store the link between device identities and group identities and they can still substitute the group identity in the NWK-DEST field before verifying the MIC. In addition, multiple overlapping groups are supported.

The properties of the solution explained above can be summarized as follows.

The sender device only requires storing a very limited amount of information.

The activities of the router device (ID2) and intermediate hops are independent of the fact if the message by the sender device (here ID1) is secured or not.

Only the group members and (of course) the router device are aware of a group G.

There is only one bit overhead in the messages (the IA bit in the NWK-INF field).

The target devices have to store the links between device IDs and group IDs which can be done efficiently.

The router device need not be trusted with application data.

These and other aspects of the invention will be further described by way of example and with reference to the schematic drawings in which:

Fig. 1 shows a Schematic example of indirect addressing

Fig. 2: Exploded view of a message at the MAC layer for a four-layer protocol stack

Fig. 3: A detailed example of indirect addressing

Fig. 4: Message formats on the MAC level during indirect addressing

Throughout the figures, same reference numerals indicate similar or corresponding features. Some of the features indicated in the drawings are typically implemented in software, and as such represent software entities, such as software modules or objects.

A solution to this problem can be found in indirect addressing (IA). Here it is assumed that a more powerful device (the router device) is available in the vicinity of the sender device. The sender device will then send a single message to the router device which will than do the repeated multicast.

This is schematically depicted in Fig. 1. The sender device ID1, member of the group G={ID1, ID3, ID4, ID5}, sends a message containing the final destination address G, its own address ID1 and a string m (i.e. the actual information to be sent to the group) to ID2, the router device. When ID2 receives the message and notices that the message coming from ID1 is intended for the group G, it will forward the message to ID3, ID4 and ID5 whose addresses it found in, for example, a pairing table.

However, problems might occur if we consider security aspects of IA. For example, the application running on ID1 generating the string m, might want to encrypt m using a cryptographic key K_G known only to members of G. Further it might want to apply a Message Integrity Code (MIC) on its own address ID1 and the destination address G in the message also using K_G. The result is that only the members of G (but *not* the router device) can read the message and receiving devices can verify if indeed the message is intended for them and if it was sent by ID1.

In many cases there is a close relation between the addresses at the APL layer and at the NWK layer which makes it possible to leave out duplicated address information in the APL layer in order to arrive at an efficient solution (address information at the NWK layer can usually not be omitted because it is required by the routing algorithms).

It is important to note that the application running on ID1 does not trust intermediate nodes (including the router ID2) with its address and message information and hence the addressing information should be protected with a MIC using the key K_G. However, the router node on the NWK level should be able to change the addressing information in order to do repeated unicast. Obviously, since G is protected by the MIC, it cannot simply be substituted by ID3, ID4 and ID5 to do repeated unicast: when the receiving devices ID3, ID4 and ID5 check the MIC, they will find a mismatch because the protected information should contain G and not ID3, ID4 or ID5, respectively. As a result, they will ignore the message.

Before going to the solution of this problem we will first give a brief review on how communication protocols are often described. Communication protocols are commonly described using a layered, OSI-like stack. For our purpose we define, from bottom to top, the physical layer (PHY), the medium access control layer (MAC), the network layer (NWK) and the application layer (APL). Roughly speaking, frames exchanged between equal layers on different devices consist of a *header* and a *payload* and a frame at level *n* in the stack is physically sent as the payload of a frame at layer *n*-1. Thus, considering the top three layers in the four-layer protocol stack that we just defined, a message sent by the MAC layer will look like depicted in Fig. 2.

Because the APL addresses are usually equal to the NWK addresses or can be derived easily, they are not always present in order to reduce the size of the message. The INF fields contain information for a receiving device on the different layers on what kind of information is present in the rest of the message and how it should be treated. For example, the MAC-INF field might indicate that the MAC-PAYLOAD is encrypted. This will show to the receiving device that it must first decrypt the payload before dealing with it further. Also, the NWK-INF field might indicate that the received frame is generated in the context of indirect addressing and should be treated accordingly.

A first embodiment further explains the invention. we give a more detailed explanation of IA including security where we will use Fig. 3 and Fig. 4. The devices ID1, ID3, ID4 and ID5 form a group G and ID1 wants to securely send a message to the other members in the group. We assume that ID1 knows the cryptographic group key K_G, the identity of the group G (but not necessarily the addresses of all the group members) and the address of its router ID2. We further assume that ID2 knows the addresses of all the members of G.

In Fig. 3, ID1 sends the message *msg1* to the router ID2 that, on the MAC level, will look something like the first message in Fig. 4 where, as compared to Fig. 2, we omitted fields that are not relevant in the current explanation. The addresses MAC-DEST and MAC-SRC indicate that a message is sent from ID1 to ID2. The addresses NWK-DEST and NWK-SRC indicate that the final destination of the message is all the members in G (possibly except ID1 itself) and that the message was sent by ID1. The NWK-INF field further indicates that we are dealing with a message in the context of indirect addressing (IA=1) and the application on ID1 encrypted the string m using the group key K_G (indicated by $E_{KG}(m)$). A dark grey background in a message means that its content is protected by a MIC using K_G (the MIC data itself is not shown in Fig. 4).

On receipt of the message from ID1, ID2 notices that it is an IA message by inspecting the IA bit in the NWK-INF field and it will perform a multiple unicast to all the members of G (again, possibly except ID1).

We will now focus on the unicast message send by ID2 with final destination ID4. From its routing information (e.g. routing tables), ID2 knows that a way to reach ID4 is sending it to ID7 after which multiple hops might follow, as indicated in Fig. 3. The message ID2 sends to ID7 on the MAC level will then look like the second message given in Fig. 4.

Note that in the NWK-DEST field, the entry G is replaced by ID4. This is required because intermediate hops are not aware of a group identity G and the unicast routing algorithms need a single, known device address as a final destination. Note further that, because of the replacement, the MIC and the protected information are no longer consistent which is indicated by the striped/light grey background of the NWK-DEST field.

After possibly more hops, a message finally ends up at ID4. If the one but last hop address was ID8 (see Fig. 3), the message will look something like the third message in Fig. 4. Now assume that ID4 knows the identity of all devices in G it can receive a message from (indicated by ID1→{G} in Fig. 3), then, by inspecting the NWK-SRC field in the received message, ID4 can obtain the group identity G. Before verifying the MIC on the message using K_G, it will replace ID4 in the NWK-DEST field by G.

The properties of the solution explained above can be summarized as follows.

- The sender device only requires storing a very limited amount of information.
- The activities of the router device (ID2) and intermediate hops are independent of the fact if the message by the sender device (here ID1) is secured or not.
- Only the group members and (of course) the router device are aware of a group G.
- There is only one bit overhead in the messages (the IA bit in the NWK-INF field).
- The target devices have to store the links between device IDs and group IDs which can be done efficiently.
- The router device need not be trusted with application data.

A second embodiment is described. Although the solution in the previous section is very efficient in simple situations, there will be problems in more complicated situations. It might be, for example, that both ID1 and ID4 are a member of G but also of a different group G' in which ID1 is also a sender device. Upon receipt of a message, ID4 is not sure if it should replace ID4 in the NWK-DEST field by G or by G' because it will have stored ID1→{G, G'}. Clearly ID4 can try all the group identities in the list belonging to ID1 until a recomputed MIC matches the MIC in the message. An alternative solution is that ID copies the group identity G in the NWK frame, for example in the NWK-INF field. This way the target devices do not have to store the link between device identities and group identities and they can still substitute the group identity in the NWK-DEST field before verifying the MIC. The cost is that in this case, the messages to be sent will be longer.

It is clear to a person skilled in the art that minor modifications to the solutions presented above still constitute the same solutions. In order to illustrate this we will present a non-exhaustive number of possible modification examples.

1. In *msg1* in Fig. 4, the identity of the router (ID2) might be omitted if it is clear from context. Receiving a message from ID1, the router might deduce from context that it must forward the message to the group G. This reduces even further the required amount of storage on the sender device and the length of the message to be sent by the sender device.

2. If the router device is only acting as router for a single device in G (in this case ID1), the sender device identity (here ID1) can be omitted from the group definition on the router device (here G={ID1,ID3,ID4,ID5}).

3. The application on the sender device (here ID1) can decide not to encrypt m but only do a MIC. In this case, $E_{KG}(m)$ in Fig. 4 will be replaced by m.

4. Rather than adding G a second time to the message, a target device might be allowed to verify the MIC under substitution of several group identities as explained in section 2.2.

5. On receipt of a message from a sender device, the router device, rather than checking the IA bit in the NWK-INF field, can also check the NWK-DEST field to conclude that the sender device sent an IA message.

6.. In the IA bit can be omitted if the group identity is repeated in the message.

7. If the target device can only receive messages from ID1 in a group context and ID1 will only send messages to the router device in an IA context, in *msg1*, G and IA can be omitted but G only *after* the MIC is computed. ID2 knows from context that it is dealing with an IA message. The target devices know from context that when they receive a message from ID1, they first have to substitute G before checking the MIC. This can be combined with 1) resulting in a very small message to be sent by the sender device (ID1).

8. The group G may consists of only two devices.

9. The router device substitutes in the NWK-DEST field the value G by ID3, ID4 and ID5, respectively, hereby ignoring the resulting inconsistency between the information protected by the MIC and the MIC itself. The router is allowed to make other modifications to the protected information as long as the target devices are capable of undoing the modifications before verifying the MIC.

11. The idea that a sender device sends a communication fragment to a router device comprising a first address reference referring to a single target device or a group of

target devices, characterized in that the address reference to the target device(s) is interpreted by the router device and used as addressing information to forward the message to the target device or target devices individually.

12. The idea in 1) where the sender device and the target device(s) share a common cryptographic key, and where the first address reference is protected under a cryptographic message authentication code computable and verifiable only by using the common cryptographic key.

13. The idea that the protected first address reference is located at a position in the communication fragment that is needed by the router device in forwarding the communication fragment to the target device(s).

14. The idea that the router device modifies the communication fragment using the interpreted address reference(s) hereby ignoring the resulting inconsistency between the communication fragment and the MIC

15. The idea that the router device replaces the first address reference by the interpreted address reference(s) hereby ignoring the resulting inconsistency between the communication fragment and the MIC.

16. The idea that a target device reconstructs the modifications made by the router device before checking the MIC.

17. The idea that a target device first substitutes the interpreted address reference by the first address reference before checking the MIC.

18. The idea that a target device obtains the information to reconstruct the message from its memory.

19. The idea that a target device obtains the information to reconstruct the message from the received message.

20. The idea that a target device obtains the first address reference from its memory.

21. The idea that a target device obtains the first address reference from the received message.

Alternatives are possible. In the description above, "comprising" does not exclude other elements or steps, "a" or "an" does not exclude a plurality, and a single processor or other unit may also fulfill the functions of several means recited in the claims.

CLAIMS:

1. Method of communication, comprising the steps of:

a sender device transferring a communication fragment to a router device,

the communication fragment comprising a first target address reference referring to a target device or group of at least one target device and

the communication fragment being at least partly protected by a MIC,

the router device forwarding and optionally modifying the communication fragment for each target device,

the router device subsequently transferring the modified communication fragment to at least one target device

characterized in that

the router device modifies the first target address reference while maintaining the original MIC,

the at least one target device receiving the modified communication fragment and restoring the original communication fragment in order to verify the MIC.

2. Sender device being arranged for transmitting a communication fragment,

the communication fragment comprising

an indirect address reference

characterized in that

for use with router device which modifies data protected by MIC, keeps original MIC,

while receiver/target device can verify MIC

3. Method or Sender device as claim 1 or 2, the communication fragment comprising a bit field to indicate the use of indirect addressing.

4. Method or Sender device as claim 3, the bit field contained in the NWK-INF field.

5. Router device being arranged for receiving a first communication fragment, comprising a first address reference referring to at least one target device, the first communication fragment at least partly being protected by a MIC, transmitting modified versions of the communication fragment to each of the at least one target devices.

6. Receiver device being arranged for receiving a modified communication fragment, the modified communication fragment protected by a MIC, recovering at least part of the first communication fragment that was used to compute the MIC and verifying the MIC.

7. System for communication comprising a sender device, router device, and receiver device as described in claim 2, 5, 6.

ABSTRACT:

In this ID we describe an efficient, secure solution for indirect addressing (IA). IA may be used, for example, in networks of which the routing algorithms are not capable of multicast but also contain very constrained devices that, although requiring multicast, are not capable of repeated unicast. This ID is useful in wireless networks containing low-power low-cost devices.

Fig. 3

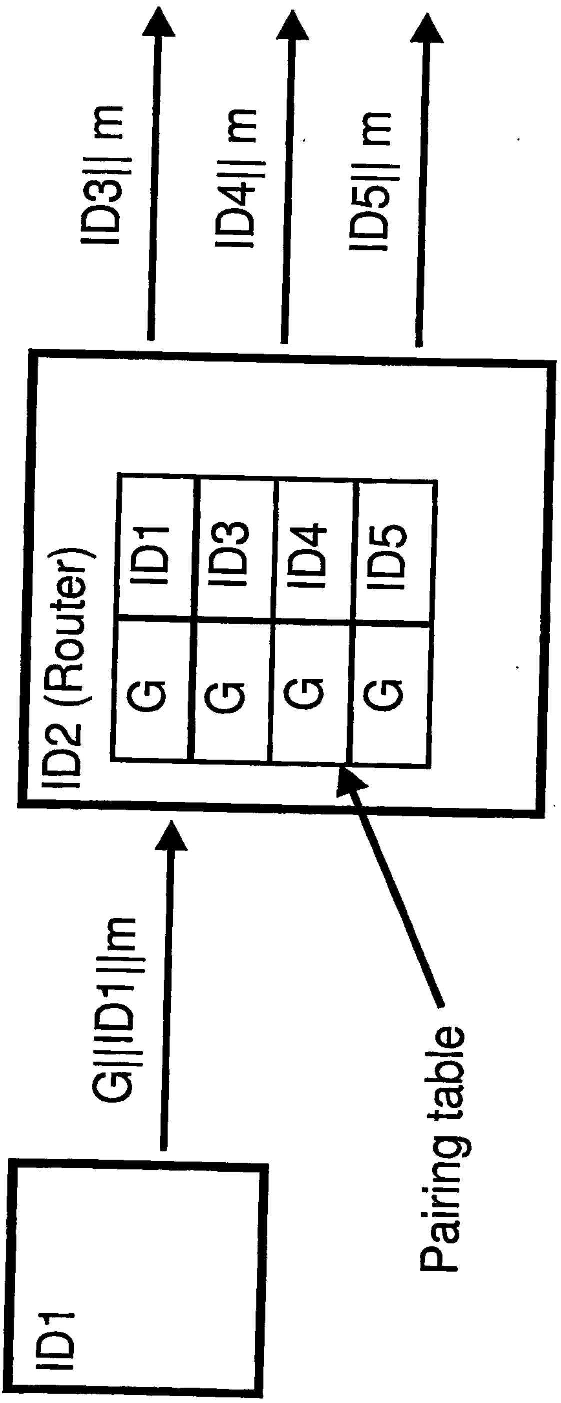
ID1
G||ID1||m
ID2 (Router)
G
ID1
G
ID3
G
ID4
G
ID5
Pairing table
ID3|| m
ID4|| m
ID5|| m

FIG.1

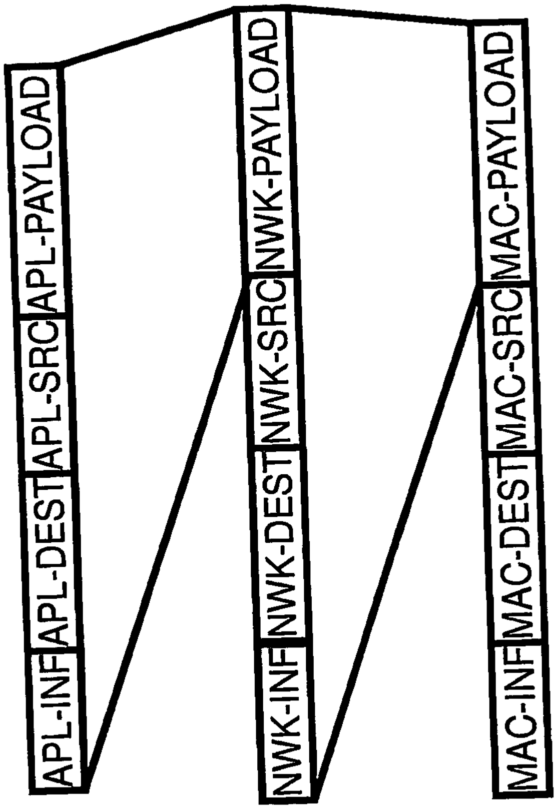
APL-INF
APL-DEST
APL-SRC
APL-PAYLOAD
NWK-INF
NWK-DEST
NWK-SRC
NWK-PAYLOAD
MAC-INF
MAC-DEST
MAC-SRC
MAC-PAYLOAD

FIG.2

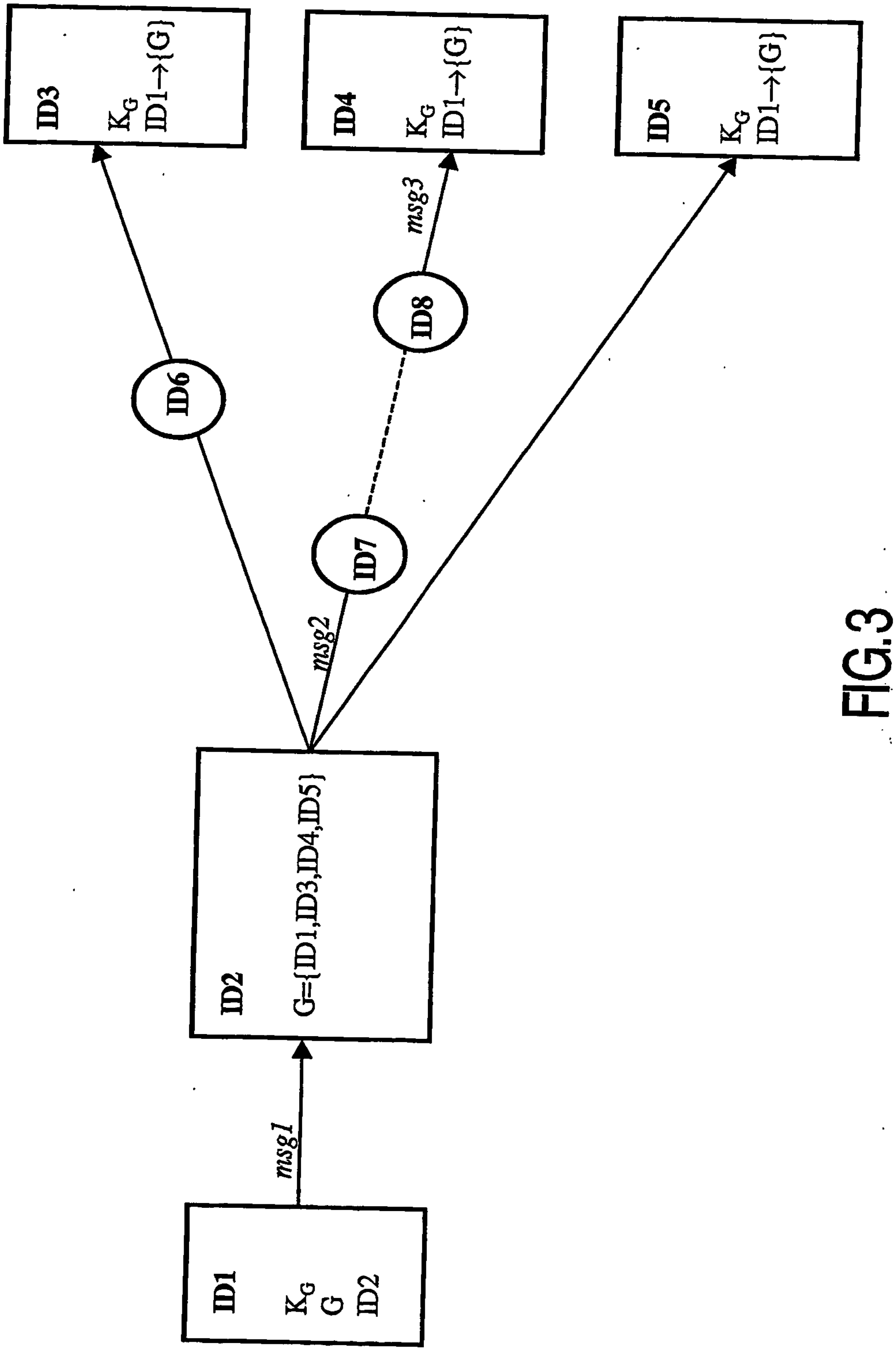
ID1
K_G
G
ID2
msg1
ID2
G={ID1,ID3,ID4,ID5}
msg2
ID6
ID7
ID8
msg3
ID3
K_G
ID1→{G}
ID4
K_G
ID1→{G}
ID5
K_G
ID1→{G}

FIG.3

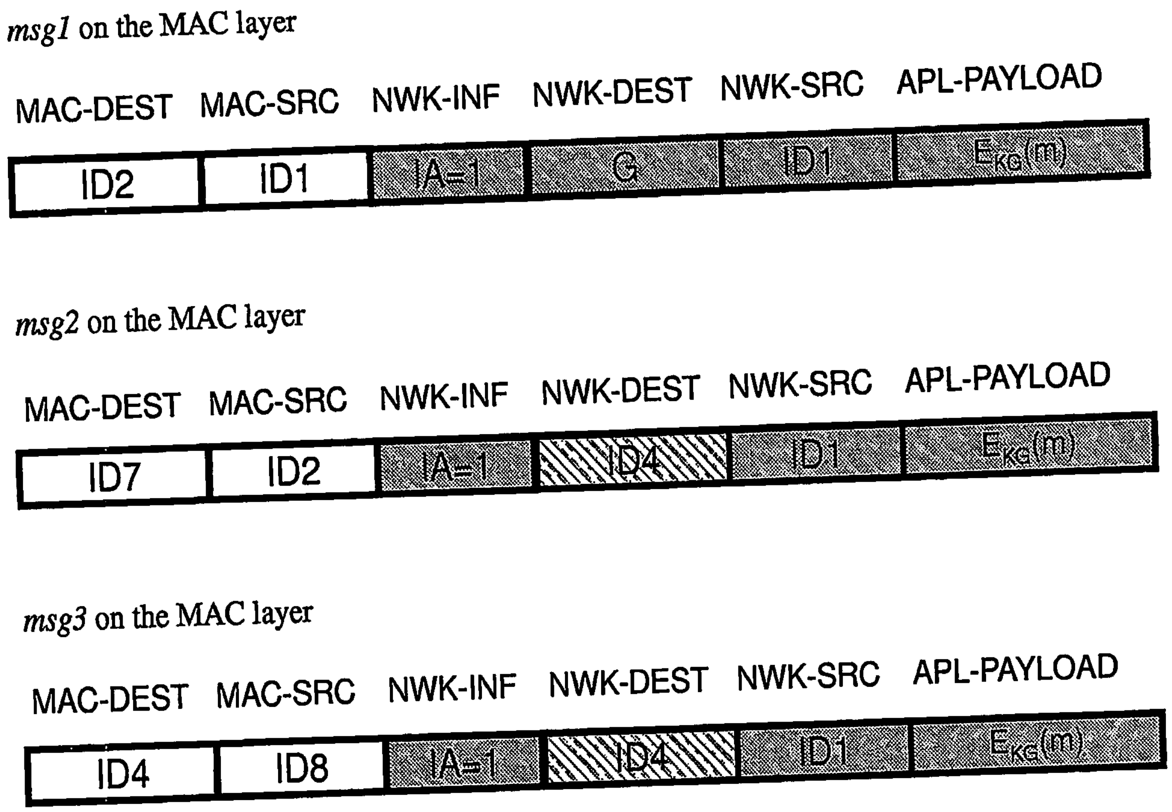
msg1 on the MAC layer
MAC-DEST
MAC-SRC
NWK-INF
NWK-DEST
NWK-SRC
APL-PAYLOAD
ID2
ID1
IA=1
G
ID1
$E_{KG}(m)$
msg2 on the MAC layer
MAC-DEST
MAC-SRC
NWK-INF
NWK-DEST
NWK-SRC
APL-PAYLOAD
ID7
ID2
IA=1
ID4
ID1
$E_{KG}(m)$
msg3 on the MAC layer
MAC-DEST
MAC-SRC
NWK-INF
NWK-DEST
NWK-SRC
APL-PAYLOAD
ID4
ID8
IA=1
ID4
ID1
$E_{KG}(m)$

FIG.4